OSINT + ARCO + PROTECCIÓN DE DATOS

MAPA-RD: Exposición y Ruta de Cierre

Así se ve tu entorno digital desde fuera. Esto es lo que hay que cerrar primero.

MAPA-RD identifica exposición real (visible públicamente), prioriza riesgos y entrega una ruta de cierre ejecututable. Incluye base operativa para gestión ARCO y un esquema mensual de control continuo.

Sin auditorías genéricas. Sin promesas vacías.

ACME Corp · Reporte RPT-2026-001 · 2026-01-11

Reporte Ejecutivo de Seguridad · Exposición pública · Confidencial

Índice de Riesgo Digital

65

RIESGO CRÍTICO

VECTORES DE VULNERABILIDAD

VEC-001

Credenciales de Base de Datos Expuestas

85 MÁXIMO

ACTIVO:	TIPO:	EXPOSICIÓN:
Base de Datos Prod (AWS RDS)	Infraestructura Cloud	Fuga en Repo Público

RUTA DE CIERRE

1. Revocar las credenciales IAM de AWS expuestas inmediatamente.
2. Rotar la contraseña maestra de la base de datos.
3. Auditar logs de CloudTrail buscando actividad sospechosa desde la fecha del commit.
4. Implementar git-secrets para prevenir futuros commits de secretos.

IMPACTO

- Compromiso total de datos de clientes (PII).
- Potencial interrupción total del servicio (Ransomware).
- Multas regulatorias severas (GDPR/Ley de Datos).

DESCRIPCIÓN DEL EVENTO

Se identificaron credenciales hardcodeadas para la base de datos principal de producción en un repositorio público de GitHub (config.js). El análisis de logs confirmó eventos de clonación no autorizados.

VEC-002

Portal de Administración sin MFA

60 CRÍTICO

ACTIVO:	TIPO:	EXPOSICIÓN:
admin.acme.com	Aplicación Web	Control Faltante

RUTA DE CIERRE

1. Forzar MFA (OTP basado en tiempo) para todos los roles administrativos.
2. Restringir el acceso solo a VPN o IPs de confianza.
3. Implementar limitación de tasa (rate-limiting) en el endpoint de login.

IMPACTO

- Acceso administrativo no autorizado.
- Manipulación o eliminación de datos.
- Instalación de puertas traseras (Backdoors).

DESCRIPCIÓN DEL EVENTO

El panel administrativo permite autenticación de un solo factor. Ataques de fuerza bruta o relleno de credenciales podrían comprometer fácilmente una cuenta de administrador.

VEC-003

Certificado SSL Desactualizado

35 MEDIO

ACTIVO:	TIPO:	EXPOSICIÓN:
dev.acme.com	Entorno de Desarrollo	Configuración

RUTA DE CIERRE

1. Aprovisionar un nuevo certificado (ej. LetsEncrypt).
2. Automatizar la renovación vía Certbot.

IMPACTO

- Disrupción del flujo de trabajo de los desarrolladores.
- Riesgo de Man-in-the-Middle (MitM) si se usa externamente.
- Pérdida de validación de confianza.

DESCRIPCIÓN DEL EVENTO

El certificado SSL para el entorno de desarrollo ha expirado, provocando advertencias en el navegador y exponiendo el tráfico a interceptación.

Anexo Técnico

Índice de Riesgo del Vector (IRV)

El **IRV** es la métrica fundamental de urgencia. No mide el riesgo teórico, sino la necesidad operativa de cierre. Se calcula internamente mediante un modelo ponderado de seis dimensiones.

FÓRMULA DE CÁLCULO

$$IRV = [\ \Sigma(Componente \times Peso)\ /\ \Sigma(Peso\ Máximo)\ ] \times 100$$

Variables del Modelo

Criticidad (CA) x4

Importancia crítica del activo para la continuidad del negocio.

Exposición (ET) x3

Ventana de tiempo y vigencia actual del hallazgo.

Superficie (SE) x3

Facilidad de acceso desde redes públicas o privadas.

Impacto (IM) x4

Suma de impactos (Financiero, Legal, Operativo, Reputacional).

Explotación (FE) x3

Recursos y complejidad técnica requerida para el ataque.

Detección (DV) x3

Probabilidad de evasión de sistemas de monitoreo.

Índice de Riesgo Digital (IRD)

El **IRD** es el indicador de postura global. Se deriva dinámicamente de los vectores activos mediante un promedio ponderado por severidad.

AGREGACIÓN PONDERADA

$$IRD = \Sigma(IRV \times Peso\ Severidad) \ / \ \Sigma(Pesos\ Severidad)$$

Matriz de Pesos

BAJO	MEDIO	ALTO	CRÍTICO	MÁXIMO
Multiplicador x1	Multiplicador x2	Multiplicador x3	Multiplicador x4	Multiplicador x5